UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/878,319	06/12/2001	Mark Crosbie	10004512-1	2127

7590 05/16/2006

IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, CO 80528-9599

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/878,319	CROSBIE ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) *11,33 and 34* is/are withdrawn from consideration.

5)☒ Claim(s) *1-10, 12-28* is/are allowed.

6)☒ Claim(s) *29-32 and 35-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to remarks filed on March 03, 2006.

Response to Arguments

2 Applicant's arguments filed on March 03, 2006, in regard to Claims 1 – 10, 12 – 32 and 35 – 43 have been fully considered.

Applicant's arguments with respect to Claims 1 – 10 and 12 – 28 are persuasive. The 35 USC 102 rejection of Claims 1 – 10 and 12 – 28 has been withdrawn.

Applicant's arguments with respect to Claims 29 – 32 and 35 – 43 are not persuasive for the following reasons:

3. Regarding independent Claim 29, applicant argued that Moran does not disclose, "if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored". This argument is not persuasive. Instant specification discloses "if a file is modified, an alert would be generated because that file is explicitly listed, even though the directory is excluded (see instant application page 36 and lines 19-20).

Moron discloses that the intrusion system monitoring a file that is in the specifically excluded directory is specifically included the file is monitored (Column 32 line 44 – Column 33 line 62 and Column 37 lines 1 – 7), wherein the Moran intrusion system iteratively checks for the modified files by comparing the location of the file against conventions for where changeable files are placed and monitor the files in conjunction with automated configuration checkers to detect changes made (by the attacker) to the configuration files. Moran further discloses that if the (system) files are modified (by an attacker) and if a deleted files are updated an alert would be generated (Column 10 lines 33 – 63).

4. Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter "if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored", broadly recited in the independent claim 29. The dependent claims 30 – 32 and 35 – 43 are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action. Accordingly, the rejection for the pending claims 29 – 32 and 35 – 43 is respectfully maintained.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 29 – 32 and 35 – 43 are rejected under 35 U.S.C. 102(e) as being anticipated by Moran (U.S. Patent Number 6,647,400).

Regarding Claim 29, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

monitoring a predetermined set of files for modifications (Column 8 lines 6 – Column 10 line 55 and Column 11 lines 16 – 54);

monitoring a predetermined set of directories for modifications (Column 8 line 6 – Column 10 line 55 and Column 11 lines 16 – 54);

generating an alert for each occurrence of a modification of a monitored file, wherein if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored, and wherein the predetermined set of files includes a system kernel file and system kernel configuration files (Column 10 lines 14 – 55; Column 13 lines 1 – 31 and Column 35 lines 9 – 42); and

generating an alert for each occurrence of a modification of a monitored directory (Column 10 lines 14 – 55; Column 13 lines 1 – 31, Column 32 line 44 – Column 33 line 62 and Column 35 lines 9 – 42).

Claim 30 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

determining which files to monitor of all files on a computer to form the predetermined set of files; determining which directories to monitor of all directories on a computer to form the predetermined set of directories (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

Claim 31 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising, for each said determining step, specifically including a file or directory, specifically excluding a file or directory or not specifically including or excluding a file or directory (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

Claim 32 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein a file or directory which is not specifically included or excluded is monitored (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

Claim 35 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes /stand/vmunix, /stand/kernel and stand/bootconf (Column 32 line 44 – Column 33 line 62).

Claim 36 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes files defining the users on a system and files used to create accounts (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 25 line 15 – Column 26 line 45).

Claim 37 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes /etc/passwd and /etc/group (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 32 line 49 – Column 33 line 11).

Claim 38 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes files which control what network services are running and which controls programs used to fulfill service requests (Column 19 lines 28 – 65 and Column 21 line 1 – 14).

Claim 39 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes /etc/inetd.conf (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 32 line 49 – Column 33 line 11).

Claim 40 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes files which are used to control the remote access of the user root without requiring a password (Column 23 lines 14 – 46 and Column 35 lines 9 – 63).

Claim 41 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes/.rhosts and /.shosts (Column 9 lines 1 – 22 and Column 35 lines 9 – 63).

Claim 42 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the set of files specifically excluded includes temporary files created by a program view (Column 27 line 32 – Column 29 line 52).

Claim 43 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of directories includes Jbin, /sbin and /usr/bin (Column 36 line 7 – Column 37 line 7 and Column 39 lines 43 – 65).

Conclusion

Allowable Subject Matter

Claim 1 – 10 and 12 – 28 are allowed.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
May 13, 2006.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100